

IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF OHIO  
IN THE EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF APPLE  
IPHONE YELLOW IN COLOR AND GRAY TCL  
FLIP PHONE, CURRENTLY LOCATED AT 410  
SOUTH HIGH STREET, COLUMBUS, OHIO  
43215

Case No. 2:25-mj-274

**AFFIDAVIT IN SUPPORT OF AN APPLICATION  
UNDER RULE 41 FOR A WARRANT TO SEARCH  
AND SEIZE**

I, **Jacob Heaberlin**, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—two electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I, Jacob Heaberlin, am a sworn law enforcement officer with the Franklin County Sheriff's Office, currently assigned as a detective with the Special Investigations Unit. I have been a deputy since 2011 and, during my tenure, have gained extensive experience in various aspects of law enforcement, including, corrections, training academy, patrol, and special investigations.

3. In 2021, I was assigned to the Special Investigations Unit (SIU), where I have conducted numerous narcotics investigations involving drug trafficking, distribution, and related criminal activity. As part of my assignment, I also serve as a federally deputized DEA Task Force Officer (TFO), working closely with federal agents to investigate high-level drug operations, executing search warrants, conducting surveillance and debriefing defendants and confidential informants. My training and

experience have provided me with extensive knowledge of narcotics trafficking methods, drug distribution networks, and indicators of illegal drug activity.

4. While assigned to SIU I conducted and participated in investigations that had a direct nexus to Mexico. Through these investigations I gained experience and understanding in the methods utilized by international drug trafficking organizations to distribute illicit narcotics.

5. The process typically begins with local traffickers, who receive bulk narcotic shipments from Mexico-based suppliers. Communication is often conducted through encrypted messaging apps, burner phones, or coded language to coordinate shipments. Once an order is placed, the supplier or their intermediary in the United States arranges for a courier to transport the narcotics. These couriers, often individuals with no direct connection to the top levels of the organization, are tasked with transporting the narcotics from a stash location or temporary holding location to various distributors.

6. The courier, usually driving a personally owned vehicle, a rental, or a vehicle registered to a fictitious person or company, retrieves the narcotics from a predetermined stash location. To evade detection, traffickers often use counter-surveillance tactics, such as multiple route changes, switching vehicles, or using third-party ride services. Upon arrival in the destination city, the courier makes drop-offs at secondary stash houses or directly to mid-level distributors. In some cases, drugs are broken down and stored in multiple locations to reduce the risk of a total loss due to law enforcement action.

7. Once narcotics are secured in the destination city, local distributors are dispatched by an individual, usually residing in Mexico, to lower-level dealers or other established customers. Often, the lower-level dealers have no contact with the courier pre or post transaction. This creates a layer of security for the couriers. Transactions are completed in high-traffic areas or at residences. Payment is typically made in cash or through peer-2-peer payment applications, or cryptocurrency. Profits are then funneled back to the Mexico-based supplier through wire transfers, money laundering operations, or bulk cash smuggling, completing the cycle of narcotics distribution.

8. This affidavit is intended to show only that there is sufficient probable cause for the requested search warrant and does not set forth all of my knowledge about this matter.

**IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

9. The property to be searched is an APPLE IPHONE YELLOW IN COLOR and a GRAY TCL FLIP PHONE, hereinafter the “Devices.” The Devices are currently located at **410 South High Street, Columbus, Ohio 43215.**

10. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

**PROBABLE CAUSE**

11. In January 2024, investigators assigned to this case identified the telephone number 1-6147499692 (\*9692) as being in contact with an identified narcotics trafficker, who resides in Mexico. To date, investigators have seized large quantities of narcotics, arrested numerous co-conspirators and completed numerous undercover narcotics purchases through the known individual in Mexico. During the investigation, investigators identified \*9692 as belonging to HERBERT.

12. In February 2024, investigators learned that HERBERT sold narcotics to a known individual, who later became a cooperating source. In subsequent interviews with the cooperating source, he/she stated that they bought narcotics from HERBERT. In March 2024, following interviews with the cooperating source, investigators conducted four controlled narcotics purchases, from HERBERT, through the cooperating source. The cooperating source communicated with HERBERT using his known phone number to complete all the transactions.

13. On May 1, 2025, a grand jury returned a four count indictment against Duke HERBERT for distribution of Fentanyl, in violation of 21 U.S.C. 841(a)(1) and 841(b)(1)(C), Conspiracy to distribute

Fentanyl, in violation of 21 U.S.C. 846, 841(a)(1), and 841(b)(1)(C), and distribution of Fentanyl Analogue, in violation of 21 U.S.C. 841(a)(1) and 841(b)(1)(B)(vi). On the same date, your Affiant received an arrest warrant for HERBERT. On May 7, 2025, your affiant, along with the assistance of the Franklin County Sheriff's Office, conducted surveillance and a traffic stop of the vehicle that was being operated by HERBERT. Following the traffic stop, HERBERT was arrested on the federal warrant in case 2-25-CR-76.

14. After securing HERBERT in the rear of a marked law enforcement vehicle, an FCSO SIU Detective deployed his K-9 partner to conduct a free air sniff around the vehicle driven by HERBERT. The K-9 alerted to the odor of narcotics coming from the vehicle. A probable cause search of the vehicle was conducted and a baggie containing approximately 4.8 gross grams of a purple powder was located between the driver's seat and the center console. No other individuals were present in the vehicle. The purple powder was field tested using a MX908 device and yielded a presumptive positive result of methamphetamine.

15. Also found in the vehicle and in HERBERT's possession were the Devices listed in this warrant. Based on training and experience and knowledge of this investigation, your affiant knows that drug traffickers, like HERBERT, utilize cellular devices to conduct their narcotics trafficking operations. From experience in reviewing data extracted from the devices of drug traffickers, your affiant expects to locate messages, through various applications, with information regarding both sources of supply of narcotics and customers who purchase narcotics from HERBERT.

16. As explained above, the Devices are currently in the lawful possession of the Drug Enforcement Administration (DEA). Therefore, while the DEA might already have all necessary authority to examine the Devices, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Devices will comply with the Fourth Amendment and other applicable laws.

17. The Devices are currently in storage at 410 South High Street, Columbus, Ohio 43215. In my training and experience, I know that the Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the DEA.

### **TECHNICAL TERMS**

18. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved

by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that

antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between

devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

19. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at [www.apple.com](http://www.apple.com) and [www.tracfone.com](http://www.tracfone.com) I know that the Devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, PDA, and they can be used to access the Internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

20. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

21. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).



- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

22. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

23. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement’s possession, the execution of this warrant does not involve the physical

intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

**CONCLUSION**

24. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

*TFO J. Heaberlin*

Jacob Heaberlin  
Task Force Officer  
Drug Enforcement Administration

Subscribed and sworn to before me  
on May 9, 2025:

*Kimberly A. Johnson*

Kimberly A. Johnson  
United States Magistrate Judge

